

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TRIANO WILLIAMS,)	
)	
Plaintiff/Counter-Defendant,)	16 C 11746
)	
vs.)	Judge Gary Feinerman
)	
AMERICAN COLLEGE OF EDUCATION, INC.,)	
)	
Defendant/Counter-Plaintiff.)	

MEMORANDUM OPINION AND ORDER

Triano Williams brought this suit against his former employer, American College of Education, Inc. (“ACE”), under 42 U.S.C. § 1981, Titles VI and VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000d *et seq.*, 2000e *et seq.*, and state law, alleging that he was discriminated against and ultimately terminated due to his race and in retaliation for complaining about discrimination. Doc. 8. ACE counterclaimed, alleging theft under Indiana law. Doc. 29. Williams then filed an amended complaint, adding allegations that ACE defamed him by publishing false allegations that he locked ACE out of its Google email account after his termination. Doc. 59.

ACE moves under Civil Rule 37(e) and the court’s inherent authority for sanctions against Williams for spoliation of evidence, charging that he intentionally destroyed electronically stored information by installing a new operating system on his ACE-issued laptop, rendering unrecoverable potentially relevant files. Docs. 90, 189. Williams denies ACE’s charge, contending that he kept a second ACE-issued laptop at ACE’s Indianapolis office, and theorizing that ACE used that laptop—or a combination of his two laptops—to fabricate evidence of the alleged spoliation. Doc. 215 at 12-15. The court held an evidentiary hearing and

entertained oral argument. Docs. 208, 210-215. Having heard, reviewed, and carefully considered the evidence, the court finds that Williams destroyed files on his laptop by installing a new operating system and committed perjury in denying that he had done so, and therefore grants ACE's sanctions motion, dismisses Williams's claims, and relinquishes its jurisdiction over ACE's counterclaim.

Background

Williams worked in ACE's Information Technology ("IT") department from 2007 through February 2016. Doc. 124-2 at ¶ 6. He was a systems administrator from 2013 through 2016. *Id.* at ¶ 8. From 2011 until his termination, Williams worked remotely from his home in Riverdale, Illinois. *Id.* at ¶¶ 10-11; Doc. 214 at 4.

On February 12, 2016, ACE told Williams that it was relocating all IT employees to its Indianapolis headquarters and that he would no longer be permitted to work remotely from home. Doc. 124-2 at ¶ 12; Doc. 212 at 68-69, 169; Doc. 124-4. Williams alleges that he was subjected to discriminatory treatment due to his race over the course of his employment and that ACE forced him to choose between relocating and leaving his job due to his race and in retaliation for his prior complaints about discrimination. Doc. 59 at ¶¶ 43-52. The most salient of those complaints were set forth in a letter (the parties call it the "ACE Culture Letter") that Williams sent to supervisors expressing his concerns that "[t]he culture of [ACE] has become very toxic ... and seems to affect only the African American demographic of our college." Doc. 124-3; Doc. 59 at ¶ 14. The letter is dated February 11, 2016—the day before ACE announced on February 12 that all IT employees had to relocate to Indianapolis—but the parties dispute whether Williams in fact prepared and sent it before February 12.

A. Williams's Knowledge of His Preservation Obligations

On February 29, 2016, ACE told Williams that it was placing him on a leave of absence and that he should no longer report to work. Doc. 124-2 at ¶ 21. Williams's attorney sent ACE a letter that day, informing it of Williams's intent to bring this suit. Doc. 89 at 10-11. ACE's counsel responded on March 10, 2016, stating:

The College asks that you remind Mr. Williams that he has affirmative obligations to preserve any and all electronic and paper documents that are relevant to his claims, his separation and his employment with the College. This not only includes preserving his company property without destruction, but also any personal email, text messages or other forms of communication that he has had with other current or former College employees. We trust Mr. Williams has and will continue to comply with [h]is preservation obligations.

Id. at 13-14.

B. Williams's Home Laptop

On February 29, 2016, the day Williams was placed on a leave of absence, ACE cut off his access to its network by changing his password and disabling his account. Doc. 212 at 54, 69, 175; Doc. 214 at 4; Doc. 124-2 at ¶¶ 21, 42. Although Williams's network access was disabled, he still could have logged into the ACE-issued laptop he kept at home by using either his previous password—because the computer was no longer on ACE's network, it would not have received the update invalidating that password—or the local administrator credentials. Doc. 212 at 70-71; Doc. 214 at 4-5. According to James Aldridge, ACE's vice president of technology, ACE could not have remotely accessed Williams's laptop after it was removed from the network. Doc. 212 at 57, 70.

On April 21, 2016, KK Byland, ACE's vice president of human resources, sent Williams a FedEx box so that he could return his ACE-issued laptop to ACE. Doc. 89 at p. 2, ¶ 5. Aldridge testified that on May 10, 2016, a receptionist delivered to his office a sealed FedEx box

from Williams containing the laptop. Doc. 212 at 80-81. IT managers Steven Carey and Rick Gehring were in Aldridge's office at the time. *Ibid.* Aldridge testified that he laid out the contents of the box—the laptop and a few pieces of bubble wrap—and photographed them. *Id.* at 81; Doc. 178-3 at 16. (Williams testified that he also sent back his power cord and keycard, neither of which appears in the photograph. Doc. 214 at 23-24; Doc. 178-3 at 16.) Aldridge did not photograph the bottom of the laptop, where the service tag (Dell's version of a serial number) was located. Doc. 212 at 118-119; Doc. 214 at 60. Aldridge then opened the laptop and turned it on, at which point he realized that it "was no longer on [ACE's] domain and that the screen was cracked." Doc. 212 at 81.

After Aldridge told Byland that he had received the laptop, she gave him a chain of custody form. *Id.* at 82. Aldridge filled out the form and then locked both the form and the laptop in his desk, using a key on his keychain. *Id.* at 82-84. The chain of custody form identifies the laptop as a "DELL Latitude E7450 wrapped in bubble wrap in a large Fedex box" with a "[v]isibly damaged screen," but does not note its service tag. Doc. 178-3 at 11. Williams testified that ACE's IT department, including Aldridge, typically identified devices by their service and asset tags. Doc. 214 at 181.

According to Aldridge, ACE's "standard procedure" when receiving a former employee's laptop was to gather the files from the laptop and provide them to the employee's supervisor, who then reviewed the files to determine whether any should be kept. Doc. 212 at 84. IT then "wipe[d] [the] computer and put a fresh image on it ... for the next user." *Ibid.* IT was unable to perform this procedure on Williams's laptop because a new operating system had been installed. *Id.* at 84-85.

Aldridge gave the laptop to Jacob Carey on May 12, 2016—a transfer he recorded on the chain of custody form, Def. Ex. 9 at 1; Doc. 178-3 at 11; Doc. 124-14 at 6—who used a bootable operating system to access the computer in search of “any additional files on the laptop that [ACE] could preserve.” Doc. 212 at 84-85. Jacob Carey accessed the laptop, changed the local administrator password, and logged in. *Id.* at 85. Upon doing so, he discovered that the laptop had been loaded with a new copy of the Windows 7 operating system and that “no files from ... Williams were present on the laptop.” *Ibid.* Jacob Carey then returned the laptop to Aldridge, who kept it locked in his desk drawer until, upon leaving ACE in January 2017, he gave it to Steven Carey. *Id.* at 87; Doc. 178-3 at 11.

In his responses to ACE’s requests for production, Williams repeatedly stated that the requested documents could be found on the laptop that he returned to ACE. Doc. 89 at 22, 36-37. For example, Williams responded to ACE’s request to produce “[a]ll documents that refer or relate in any way to your employment with [ACE], including but not limited to, time records, policies, procedures, and personnel documents” by stating: “These documents were maintained electronically and were accessed via my laptop which was returned.” *Id.* at p. 22, ¶ 1. Williams gave a similar response—“Documents that may have been contained on my laptop are now unavailable.”—to ACE’s requests for “[d]ocuments relating to any communications, including but not limited to e-mails and text messages,” between Williams and Rommel Haynes, Dr. Linetta Durand, Amber Ying, or “any person not employed by [ACE] regarding the allegations in the Complaint.” *Id.* at pp. 36-37, ¶¶ 60-63. And Williams gave that same response to ACE’s request for documents “reflecting [his] job duties and responsibilities while he was employed by [ACE]” and documents related to his attempts to obtain employment after he left ACE. *Id.* at p. 37, ¶¶ 65-66.

C. D4/Evans's Forensic Analysis

ACE sent Williams's laptop to John Evans, a computer forensics expert with the firm D4, LLC, to perform a forensic analysis. Doc. 214 at 29-31; Doc. 89 at 94. D4 received the laptop and ACE's chain of custody form in July 2017. Doc. 214 at 31. Evans testified that the laptop received by D4 matched the description on the chain of custody form. *Ibid.* The shipping label identified the sender as Steven Carey, as did the form. Doc. 178-2 at 7, 13. Evans testified that D4 never received any other computers from ACE, and that D4 examined only one laptop: a Dell Latitude E7450 with service tag CXF4M32 received from ACE. Doc. 214 at 31-32, 41. Byland testified that the laptop Williams returned to ACE was the one that ACE sent to Evans and that she had no reason to believe that anyone had altered or tampered with it. Doc. 212 at 177.

Evans performed a forensic examination on the laptop and found that the operating system had been reinstalled on March 28, 2016. Doc. 214 at 32. Evans added that the previous operating system had been installed on June 1, 2015. *Id.* at 42. Evans testified that reinstallation requires human intervention in the form of "affirmative actions to click through screens to set up the new operating system." *Id.* at 37. In Evans's experience, reinstalling an operating system is a common method of deleting information from a computer. *Ibid.* He explained that when an operating system is reinstalled, files that were deleted before the reinstallation can be overwritten, making them unrecoverable. *Id.* at 32.

Evans found evidence that the reinstallation of the operating system on Williams's laptop had that effect. *Id.* at 33. Specifically, he found "evidence of at least 20 files that were opened prior to the reinstallation"—and thus "were present on the hard drive at that time"—but that "no longer exist[ed] on the device" when he examined it. *Ibid.* Evans testified that he was unable to recover any autosaved Google login information or any email communications other than those

saved in Outlook (and therefore available independently through Outlook). *Id.* at 32-33, 46.

When Evans received the laptop, it did not appear to be associated with any domain or physical network. *Id.* at 35.

According to Evans, reinstalling the operating system moves the previous operating system and user profiles—which Evans described as “a collection of documents related to logs on that computer”—to a “windows.old” folder. *Id.* at 34. Evans found six user profiles that pre-dated the reinstallation: “Administrator,” which accessed the device from June 2015 through March 2016; “Jose.Rubio,” which accessed the device in July 2015; “Triano.Williams,” which accessed the device from August 2015 through January 2016; “Triano.Williams.ACE,” which accessed the device from January through February 2016; and two profiles with no activity (“Default” and “Public”). *Id.* at 34-36, 48; Doc. 89 at 95. From August 2015 through February 2016, the only profiles with any activity were “Triano.Williams” and “Triano.Williams.ACE.” Doc. 214 at 36. The only profiles present after the operating system reinstallation were “ACE,” “Default,” “Public,” and an “Administrator” profile deleted shortly after the reinstallation. *Id.* at 37; Doc. 89 at 95.

Evans found evidence of activity on the previous operating system on March 4, March 9, and March 28, 2016. Doc. 214 at 34. That activity included opening about twenty files on March 28, 2016, the date of the reinstallation. *Id.* Because none of those files were present on the laptop after the reinstallation, Evans concluded that they had been deleted before the reinstallation. *Id.* at 34-35. Evans was able to determine the names of the deleted files but not their contents, *id.* at 66-67, and observed that the names of files do not necessarily match their contents, *id.* at 82-83. Evans also found that USB devices were connected to the laptop on February 29 and March 3, 2016. *Id.* at 36. Evans did not find any documents or activity from

after the reinstallation. *Id.* at 37. Evans found the TeamViewer application (a mechanism for obtaining remote access to a computer) and the logs it generated when used, but he did not find any evidence of TeamViewer activity after February 1, 2016, nor did he find any other evidence of remote access in connection with the March 28, 2016 reinstallation. *Id.* at 36, 44; Doc. 178-2 at 4. Evans testified that as far as he knows, it is not possible to reinstall an operating system remotely. Doc. 214 at 76. If it were possible to do so, Evans would expect the process to leave behind evidence, but he did not find any. *Id.* at 79.

Evans recovered more than 10,000 deleted items, which he opined were recoverable only through forensic means. *Id.* at 41. Evans opined that all the items were deleted from the laptop he examined. *Ibid.* He added that “it is impossible to tell what information was overwritten, and therefore no longer recoverable, as a result of the” reinstallation. Doc. 178-2 at 3.

Evans looked for evidence of tampering beginning on May 10, 2016—when ACE received the laptop from Williams—but found none. Doc. 214 at 38. Evans found nothing on the laptop that was altered after May 12, 2016, when Jacob Carey used a boot disk to start the computer and reset the password. *Id.* at 37, 47; Doc. 178-3 at 18-19. Evans found two files consistent with the activity that Jacob Carey described, both dated May 12, 2016. Doc. 178-2 at 5, 19-21. Evans testified that he would expect to find evidence of doctoring if someone had tried to make a laptop look like someone else was using it. Doc. 214 at 38.

D. Protek/Glud’s Forensic Analysis

Williams hired Protek International, Inc. to analyze a copy of the forensic image that D4 had made of his laptop. Doc. 169-2 at 1. Like Evans, Protek found that the “active operating system” was installed March 28, 2016, likely by way of reinstalling Windows, as evidenced by the presence of the “Windows.old” folder. *Id.* at 2. Protek found a few dozen emails to or from Williams’s personal accounts. *Ibid.*; Doc. 169-1 at ¶ 9. (Evans testified that Protek’s finding

those emails is not inconsistent with his conclusion that there were no recoverable emails because Evans searched for locally saved emails, not for emails available in Outlook. Doc. 214 at 46; Doc. 178-2 at 5.) Protek did not find the two files that Jacob Carey said he renamed—“Utilman.exe” to “Utilman.exe.old,” and “cmd.exe” to “Utilman.exe”—while attempting to access the laptop with a boot disk, but Protek did find evidence that a program file named “Utilman.exe” was last run on May 10, 2016. Doc. 169-2 at 3.

Protek found “[s]everal versions of spreadsheets tracking ACE computer assets.” *Ibid.* Protek also examined “ShellBag” and “UserAssist” artifacts, which can provide information about user activity. *Ibid.* Protek determined that the ShellBag data, which “help[] track the views, sizes and positions of a folder when displayed on a monitor screen” and thus offer “insight into the folder/browsing history of a user,” provided “evidence of network access to resources attributable to Higher Education Holdings”—ACE’s holding company—from June 3, 2015 through January 6, 2016. *Ibid.* Protek also determined that the UserAssist artifacts, which record “programs executed by a user account,” showed activity on the same profiles and in the same time periods as Evans had found. *Compare ibid., with* Doc. 214 at 34-36, 48, *and* Doc. 89 at 95.

At the evidentiary hearing, Williams asked Evans whether a spreadsheet Protek prepared of the UserAssist data, Pl. Exs. 12, 22; Doc. 169-2, contained evidence of remote access to Williams’s laptop on March 28, 2016. Doc. 214 at 84-87. Evans opined that even assuming that the UserAssist spreadsheet was accurate, it showed only that a program named “Remote Desktop Connection” was run on the laptop after the reinstallation, not that the laptop was in fact accessed remotely from another device. Doc. 214 at 87-89. (Although Plaintiff’s Exhibit 22 was

not separately admitted at the evidentiary hearing, it is a reproduction of Exhibit D to Protek's report, Doc. 169-2; Pl. Ex. 12, which Williams filed in its native (Excel) format on a USB drive.)

Todd Glud, Protek's director and senior consultant for electronic discovery and computer forensics, opined that ACE's chain of custody form was deficient because it did not "record any unique identifying information," such as a service tag, that would distinguish Williams's laptop "from other laptops of the same make and model." Doc. 169-1 at ¶¶ 1, 6. (ACE's motion to strike Glud's opinions about the chain of custody form, Doc. 163, is denied as moot because those opinions do not affect the outcome of ACE's spoliation motion.) Glud also opined that one of the inventory spreadsheets on the forensic image of Williams's laptop indicated that "two Dell Latitude E6430 laptop computers" were at some point assigned to Williams, both with service tags different from the tag on the E7450 laptop that D4 analyzed. Doc. 169-1 at ¶ 8. Williams averred in a declaration that the laptop he returned to ACE from his home and the laptop he used at the Indianapolis office (of which more in a moment) were E7450s. Doc. 180-15 at ¶¶ 8, 31-32.

Evans prepared a supplemental report in response to Protek's findings and Williams's declaration. Doc. 178-2 at 2. Evans opined that Protek's findings were largely consistent with his own. *Id.* at 4-5. Evans agreed with Glud that the inventory documents referred to two E6430 laptops, but found that none of the documents referred to the service tag of the laptop that D4 imaged. *Id.* at 5. Ultimately, Evans opined that Protek's findings were "consistent with D4's conclusion that the reinstallation of the operating system may have caused the permanent deletion of ... potentially relevant information." *Id.* at 6. Given the lack of evidence of remote access and the affirmative steps required to accomplish reinstallation, Evans opined that "the

reinstallation of the operating system, creation of the ACE user account, and deletion of the administrator user account were completed locally on March 28, 2016.” *Ibid.*

E. Williams’s Denials of Having Installed a New Operating System

At his deposition, in his declaration, and at the evidentiary hearing, Williams denied having installed a new operating system on his laptop before returning it to ACE. Doc. 89 at 86 (p. 156, ll. 17-19); Doc. 180-15 at ¶ 4; Doc. 214 at 147. At the evidentiary hearing, Williams also denied having deleted any documents “pertaining to this litigation.” Doc. 214 at 172. Williams admitted that, before returning the laptop, he deleted personal files like “pictures of [his] daughter and family activities and things like that” and possibly “a couple of court [child] custody document things.” *Id.* at 132, 172.

Williams testified that if he had wanted to delete information from the laptop, he would have reimaged it or “done a shred.” *Id.* at 147-148. Evans acknowledged that there are more effective ways to delete data from a laptop than reinstalling the operating system, such as physically destroying the hard drive or using a tool designed to wipe a hard drive. *Id.* at 69-70. Evans did not find any evidence that those methods were used on the laptop. *Id.* at 70.

Williams also testified that while the reinstalled operating system was set to Pacific time, he “always” sets up computers with Central time. *Id.* at 148 (“It’s automatic with me.”). Moreover, Williams testified that his laptop contained “no documents regarding [racial] discrimination” at ACE because he discussed his concerns with coworkers only in person, on the phone, or through instant messaging. *Ibid.*

When presented at the evidentiary hearing with the laptop that Aldridge identified as the one he received from Williams, Doc. 212 at 81-82, and that Evans identified as the one he received from ACE, Doc. 214 at 30-31, Williams said that he was not sure whether that laptop was in fact the one he returned to ACE, but that he did not think it was, *id.* at 169-170. Williams

explained that although the laptop was the same model as the one he returned, it had an asset tag that either was not on the laptop he returned or was in a different location, and that it had neither the webcam cover that he put on “just about every one of [his] laptops that ever had a web cam on it” nor the “stickiness” that removing the webcam cover would have left behind. *Ibid.*

F. ACE’s Network and IT Migration

ACE used an “image”—which Aldridge described as “a picture of an operating system, its applications and configuration,” “kind of like an initial print” that can be “replicate[d] ... over and over again”—to standardize how employee laptops were configured. Doc 212 at 62.

Aldridge testified that the only image in use during his time at ACE (from November 2015 through January 2017, *id.* at 57) was one created by Jose Rubio. *Id.* at 63-64. Rubio worked for ACE’s sister company, Academic Partnerships, to which ACE originally contracted its IT functions. *Id.* at 49, 63. Edward McGory, vice president of information technology at Higher Education Holdings (as noted, ACE’s holding company), testified that because Rubio created the image, his profile appeared on any computer configured using that image unless the profile was manually deleted. *Id.* at 191. Accordingly, McGory explained, the appearance of Rubio’s profile on a laptop does not necessarily mean that Rubio accessed the device. *Ibid.*

ACE began taking over its IT functions from Academic Partnerships in 2015 and completed the migration sometime in 2016. *Id.* at 49-51. Aldridge testified that, as part of the migration, ACE created a new image in mid-2016. *Id.* at 102-103. He testified that Jacob Carey created the new ACE image and that he was not aware of Williams ever creating a new image. *Id.* at 102-103, 106. Williams and his coworker Haynes, by contrast, testified that Williams created a new image after the migration. Doc. 214 at 104, 140. Williams testified that he did so by July or August 2015, when he first received the laptop he kept at home, and therefore that Rubio’s profile was never on that device. *Id.* at 140-141.

Whenever a user logged in to one of ACE's computers for the first time, the computer created for that user a "profile," which is a folder holding "that person's documents, settings, those sorts of things." Doc. 212 at 63, 190. In December 2015, ACE switched from the Higher Education Holdings domain to its own domain as part of the migration of IT functions away from Academic Partnerships. *Id.* at 50, 64. Whenever a user logged in to an ACE computer for the first time after the domain change, the computer created a new profile under the new ACE domain. *Id.* at 64, 190. IT then moved the user's files and settings to the new profile, and the old profile remained on the computer unless it was manually deleted. *Id.* at 64, 190-191. Aldridge testified that both before and after the domain change, Rubio's profile appeared on the laptops that had been configured with the image Rubio created. *Id.* at 104-105.

Williams testified that his profile would have appeared on several ACE laptops because he logged in while performing repairs on those devices. Doc. 214 at 12-13.

McGory testified that Windows login credentials could not have been autosaved on an ACE-issued laptop such that anyone with physical access to the device could log in, and that IT administrators could change but not view a user's network password. Doc. 212 at 181, 186-187. According to McGory, any ACE employee could access any laptop connected to the ACE network using that employee's own credentials. Doc. 212 at 187. An employee who logged into another user's laptop would gain access to the applications on the device, and a profile would be created on the laptop for that employee, but the employee would not be able to access other users' profiles. *Ibid.* Accessing information that a user saved locally on a given device would thus require both the physical device and the user's credentials. *Id.* at 188.

G. The Second Laptop

Williams testified that, in addition to the ACE-issued laptop he kept at home and sent back to ACE, he had a second laptop that he used when working at ACE's Indianapolis office.

Doc. 214 at 8. Williams testified that he used the Indianapolis laptop to remotely access the ACE laptop he kept at home. *Id.* at 142; Doc. 132-10 at ¶ 21. Williams testified that the Indianapolis laptop “was one of the ones [he] let people use” as spares when their assigned laptops were being repaired. Doc. 214 at 8. He testified that although he loaned that laptop to others, “it wasn’t a loaner to [him],” but rather was “the computer that [he] had previous to” the one he kept at home and that was “still assigned” to him. *Id.* at 10. Williams did not put his name on the Indianapolis laptop. *Id.* at 16. The last time Williams worked from the Indianapolis office was in November or December 2015. *Id.* at 16-17.

According to Shawntel Landry, ACE’s president, it was ACE policy to assign each employee only one laptop. Doc. 212 at 20. Aldridge and Byland testified that they were not aware of anyone being assigned two laptops at the same time. *Id.* at 88, 140-141. The IT department sometimes maintained a stock of loaner computers in the Indianapolis office. *Id.* at 43-44, 99, 158. Haynes testified that the loaners were kept along with other spare equipment in a service closet or server room. Doc. 214 at 101. Aldridge testified that the loaners were given out as spares to employees whose assigned laptops were being repaired. Doc. 212 at 99.

Byland testified that she first learned in Fall 2018, nearly two years into this litigation, that Williams claimed to have been assigned more than one laptop. *Id.* at 141-142. ACE searched without success for additional laptops that had been assigned to Williams. *Id.* at 142. Byland testified that because she did not know in 2016 that Williams had used any other devices, the only device she preserved for discovery was the laptop he returned in May 2016. *Ibid.*

Williams acknowledged that he did not disclose the existence of his second laptop during discovery, explaining that he “didn’t think about that computer” until he saw that Evans had found Rubio’s profile on the laptop sent to D4—a profile that Williams thought would not have

appeared on the laptop he returned to ACE. Doc. 214 at 8-9. When asked at his deposition, “Do you have any other computers in addition to that laptop computer that you returned to ACE?”, Williams testified, “I have my personal computer” and did not mention any second ACE-issued computer in Indianapolis. Def. Ex. 16; Doc. 214 at 186. At the evidentiary hearing, Williams gave this explanation for why he testified at his deposition that he had only one ACE-issued computer, the one he used at home and returned to ACE:

I didn’t think about any other devices at that point because I didn’t use it on a regular basis. So, when we were talking about what was going on at the time, I was only thinking about the one that I currently had at home that I sent back.

... .

My personal computer had nothing to do with ACE, so when I said I had my personal computer, that’s what I said. And as I just stated, I wasn’t thinking about the second laptop that I left in Indiana.

Doc. 214 at 185-186.

Williams testified that, in addition to the Pacific time zone setting and the presence of Rubio’s profile on the laptop that D4/Evans examined, ShellBag artifacts he understood to have been found on the forensic image of that laptop and included in Protek’s report led him to think that the imaged laptop was not the one he returned, which in turn reminded him about the Indianapolis laptop. Doc. 214 at 158-159. Specifically, Williams interpreted the ShellBag data to indicate that Gehring and Dan Holstein had used the imaged laptop, reasoning that the data reflected that someone had accessed their network folders and Williams did not have access to those folders. *Id.* at 159-160. (Williams’s testimony was offered only to explain what made him think that the imaged laptop was not the one he had returned, and not for the truth of his interpretation of the ShellBag data. *Id.* at 157-158.) Williams testified that he reviewed the ShellBag data when he reviewed Protek’s November 13, 2018 report, *id.* at 149-151; Doc. 169-2,

about three months after he first averred in an August 6, 2018 declaration that he had a second laptop that was kept in Indianapolis, Doc. 124-2 at ¶¶ 43-45.

Evans testified that ShellBag is “a forensic artifact that is related to windows that are open and preset on a Windows computer, and where those folders may point.” Doc. 214 at 72. Evans opined that ShellBag entries “evidence the location of folders that were accessed” but do not provide information about who accessed the folders. *Id.* at 72-74. According to Evans, ShellBag entries mentioning Gehring and Holstein indicated that someone using the laptop accessed network folders associated with Gehring and Holstein, and not that they personally used the laptop. *Id.* at 72-75.

Williams testified that, in his experience, it is “pretty easy” to remove and replace a laptop’s physical screen, even for somebody without a technical background. *Id.* at 182. Williams estimated that it would take an experienced person about fifteen minutes with a small Phillips head screwdriver, while an inexperienced person working from a how-to video might need thirty minutes to an hour. *Ibid.*

Aldridge testified that he never altered any device to make it look like it was Williams’s laptop, never used Williams’s credentials to log into any device, never sent emails or instant messages from Williams’s laptop, and never downloaded a new operating system onto Williams’s laptop. Doc. 212 at 89. Aldridge also testified that he was not aware of Williams ever using multiple devices in the Indianapolis office or of anyone else having access to the laptop Williams returned to ACE other than the people on the chain of custody form. *Id.* at 89-90. Byland testified that she never removed Williams’s laptop from Aldridge’s drawer, accessed it with Williams’s credentials, altered the laptop in any way before sending it to Evans, altered any other device to make it look like it belonged to Williams, instructed anyone else to alter a

device, directed anyone to send any other computers to Evans, or directed anyone to add files to the laptop Williams returned. *Id.* at 147-148.

When, after leaving ACE, Williams received phone calls from ACE employees who said that he was appearing as available on Skype for Business, he reported the problem to Byland. *Id.* at 172-173; Doc. 214 at 175-176. Byland referred the issue to Aldridge, Doc. 212 at 173-174, who told her that Williams's Skype for Business account was disabled the day he left ACE and that his network access was cut off, Doc. 214 at 210-212; Def. Ex. 18. Williams testified that this issue arose after he returned his laptop, Doc. 214 at 176, but in fact he emailed Byland about it on March 10, 2016, Pl. Ex. 26, well before he returned the laptop in May 2016.

H. Remote Access

As noted, Williams maintains that he did not reinstall the operating system on his home laptop; instead, he suggests someone at ACE remotely accessed that laptop and performed the reinstallation. Doc. 215 at 15. ACE's IT team used TeamViewer, a program that allowed IT employees providing technical support to remotely access a user's desktop. Doc. 212 at 64-65. Aldridge testified that *two* people are required to initiate a TeamViewer session: the user seeking support must provide a session ID and password, and the IT employee must remotely enter those credentials to complete the connection. *Id.* at 65 ("Without [the credentials], you can't just remote desktop in to anybody's computer at will."). Aldridge testified that TeamViewer generates a new password for each session, and that he had never seen it configured so that the password would stay the same across sessions. *Id.* at 107. McGory testified that TeamViewer cannot be used to remotely access a device unless the device is powered on and connected to the internet and the TeamViewer application is running. *Id.* at 188-189.

Haynes testified that when one laptop is used to remotely access another, the second laptop's files are not transferred to the first laptop unless the user manually moves a file from one computer to the other. Doc. 214 at 119.

Williams testified that he set up TeamViewer on his home laptop so that the password would stay the same each session, allowing him to connect to that laptop from his second laptop in Indianapolis so long as the one at home was turned on and had TeamViewer installed. *Id.* at 9. Evans opined that it could have been possible to remotely access Williams's laptop without his cooperation. *Id.* at 77.

I. ACE's Google Account and Williams's Deletion of Emails

ACE had a student email account hosted by Google. Doc. 212 at 20. In May 2016, ACE began receiving complaints from students who said that they were locked out of their individual email accounts. Doc. 212 at 21, 53. ACE discovered that it was locked out of the account and that Williams was still listed as the administrator. *Id.* at 21.

At some point after Williams returned his laptop to ACE, Aldridge asked him for help accessing the Google account. Doc. 214 at 6-7. Williams told Aldridge that his administrator password was autosaved on the returned laptop and that he would be willing to help if Aldridge sent the laptop back to him. Doc. 212 at 115. Williams testified that he did not know the password. Doc. 214 at 133. Aldridge did not return the laptop to Williams because "[t]here was no data on the computer for [Williams] to retrieve at that time." Doc. 212 at 115. Williams testified that his Google credentials were also autosaved on the laptop he kept in the Indianapolis office. Doc. 214 at 5. Williams further testified that he did not tell Aldridge about the laptop in Indianapolis because he "didn't think about it." *Id.* at 7-8.

ACE believed, based on records from Google, that the recovery email address for its Google account was "trianoaw09@live.com," Williams's personal email address. Doc. 212 at

24; Doc. 214 at 197. In a February 21, 2018 letter responding to ACE’s concerns with Williams’s discovery responses, his counsel stated that Williams “has not saved emails back to 2007 as he has them on auto delete every 30-90 days and in addition, [he] cleans out his emails on a regular basis. Also, [Williams] does not retain text messages as it affects the storage and function of his phone.” Doc. 89 at 80-81.

J. The ACE Culture Letter

Byland testified that she received the ACE Culture Letter—which, as noted, was dated February 11, 2016—on February 23, 2016, eleven days *after* the February 12, 2016 team meeting in which ACE asked all its IT employees to relocate to Indianapolis. Doc. 212 at 169. Williams, however, testified that he sent the letter shortly *before* ACE told him about the relocation. Doc. 214 at 128. Neither Evans nor Protek found the ACE Culture Letter on Williams’s laptop, except for the copy Williams attached to an email (whose date is not apparent from the record) that he sent to Aldridge, Byland, and Landry. Doc. 89 at 96; Doc. 169-2 at 2-3.

Discussion

ACE seeks sanctions for Williams’s alleged spoliation—reinstalling his ACE-issued laptop’s operating system and thereby rendering unrecoverable the files that had been deleted before the reinstallation—under Rule 37(e) and the court’s inherent authority. Rule 37(e) permits sanctions “[i]f electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery.” Fed. R. Civ. P. 37(e). If the court “find[s] prejudice to another party from loss of the information,” it “may order measures no greater than necessary to cure the prejudice.” Fed. R. Civ. P. 37(e)(1). However, if the court “find[s] that the party [responsible for not preserving the information] acted with the intent to deprive another party of the information’s use in the litigation,” it may:

“(A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment.” Fed. R. Civ. P. 37(e)(2).

Aside from its Rule 37 authority, the court has the inherent “ability to fashion an appropriate sanction for conduct which abuses the judicial process.” *Chambers v. NASCO, Inc.*, 501 U.S. 32, 44-45 (1991); *see also Roadway Express, Inc. v. Piper*, 447 U.S. 752, 765 (1980) (describing the “well-acknowledged inherent power of a court to levy sanctions in response to abusive litigation practices”) (internal quotation marks omitted). “Sanctions imposed pursuant to the district court’s inherent power are appropriate where a party has willfully abused the judicial process or otherwise conducted litigation in bad faith.” *Tucker v. Williams*, 682 F.3d 654, 661-62 (7th Cir. 2012); *see also Ramirez v. T & H Lemont, Inc.*, 845 F.3d 772, 776 (7th Cir. 2016) (same). That power is “permissibly exercised not merely to remedy prejudice to a party, but also to reprimand the offender and to deter future parties from trampling upon the integrity of the court.” *Salmeron v. Enter. Recovery Sys., Inc.*, 579 F.3d 787, 797 (7th Cir. 2009) (internal quotation marks omitted).

“Because of their very potency, inherent powers must be exercised with restraint and discretion.” *Chambers*, 501 U.S. at 44; *see also Mach v. Will Cnty. Sheriff*, 580 F.3d 495, 502 (7th Cir. 2009) (“A district court should be cautious when exercising such inherent authority.”). The inherent power should be used “sparingly, to punish misconduct (1) occurring in the litigation itself, not in the events giving rise to the litigation ... , and (2) not adequately dealt with by other rules.” *Zapata Hermanos Sucesores, S.A. v. Hearthside Baking Co.*, 313 F.3d 385, 391 (7th Cir. 2002); *see also Chambers*, 501 U.S. at 50 (“[W]hen there is bad-faith conduct in the course of litigation that could be adequately sanctioned under the Rules, the court ordinarily

should rely on the Rules rather than the inherent power.”); *United States v. Rogers Cartage Co.*, 794 F.3d 854, 863 (7th Cir. 2015) (declining to affirm the district court’s sanctions order on the basis of the court’s inherent authority because “Rule 11 was adequate for the court’s purposes”). “But if in the informed discretion of the court, neither [a] statute nor the Rules are up to the task, the court may safely rely on its inherent power.” *Chambers*, 501 U.S. at 50. The inherent authority is properly exercised where “conduct sanctionable under the Rules was intertwined within conduct that only the inherent power could address,” as “requiring a court first to apply Rules and statutes containing sanctioning provisions to discrete occurrences before invoking inherent power to address remaining instances of sanctionable conduct would serve only to foster extensive and needless satellite litigation, which is contrary to the aim of the Rules themselves.” *Id.* at 51. Accordingly, “the inherent power of a court can be invoked even if procedural rules exist which sanction the same conduct.” *Id.* at 49; *see also Mach*, 580 F.3d at 502.

“[O]utright dismissal ... is a particularly severe sanction, yet is within the court’s discretion” under its inherent authority. *Chambers*, 501 U.S. at 45. The court may invoke its inherent authority to “dismiss a case for discovery violations or bad faith conduct in litigation,” *Greviskes v. Univs. Research Ass’n*, 417 F.3d 752, 758 (7th Cir. 2005), so long as dismissal is “proportionate to the gravity of the offense,” *Montano v. City of Chicago*, 535 F.3d 558, 563 (7th Cir. 2008). Significant here, “[a]s a fraud on the court, perjury may warrant the sanction of dismissal.” *Id.* at 564. The Seventh Circuit does “not require a district court to measure the impact on the litigation of a wrongdoer’s willful misconduct before it issues a dismissal sanction,” *Salmeron*, 579 F.3d at 797, but still the court must “find that the responsible party acted or failed to act with a degree of culpability that exceeds simple inadvertence or mistake before it may choose dismissal as a sanction for discovery violations,” *Ramirez*, 845 F.3d at 776.

“In civil cases, the facts underlying a district court’s decision to dismiss the suit or enter a default judgment as a sanction under Rule 37 or the court’s inherent authority need only be established by a preponderance of the evidence.” *Id.* at 781.

Williams concedes that he had a duty to preserve the files on the ACE-issued laptop he kept at home. Doc. 124 at 16, 22. And Williams does not dispute that the forensic image created by Evans shows that someone reinstalled the operating system on the laptop Evans examined, rendering unrecoverable many files that had been deleted from the laptop before the reinstallation. But Williams offers two theories as support for the proposition that he did not reinstall the operating system: (1) Evans examined a laptop different from the one Williams returned to ACE; and/or (2) someone else reinstalled the operating system on the laptop Evans examined and tried to frame Williams for the resulting spoliation. Doc. 215 at 12-17.

I. Williams’s Willful Spoliation of Evidence

To prevail under Rule 37(e)(2) or the court’s inherent authority, ACE must show by a preponderance of the evidence that Williams engaged in spoliation with the requisite intent. The evidence here more than meets that standard.

A. Spoliation

ACE’s version of events is supported by the record, and it proceeds as follows. Williams returned his ACE-issued laptop to ACE in May 2016. Doc. 214 at 5. Aldridge credibly testified that he received the laptop, turned it on, and discovered that the screen was damaged and the laptop was no longer on ACE’s domain. Doc. 212 at 80-81. Aldridge gave the laptop to Jacob Carey, and Carey discovered that the operating system had been reinstalled and that he could not find any of Williams’s files. *Id.* at 84-85. Aldridge credibly testified that he then kept the laptop locked in his desk drawer until he left ACE in January 2017, at which point he gave it to Steven Carey. *Id.* at 87. Steven Carey sent the laptop to D4 in July 2017. Doc. 178-2 at 7, 13; Doc. 214

at 31. Evans credibly testified that the laptop D4 received from ACE matched the description on the chain of custody form and that it was the only device for which he prepared a forensic image. Doc. 214 at 31-32, 41.

Protek conducted its analysis using the forensic image that Evans had created. Doc. 169-2 at 1. Both Evans and Protek found that the laptop's operating system was reinstalled on March 28, 2016—while the laptop was in Williams's possession. Doc. 214 at 32; Doc. 169-2 at 2. Evans found (and Protek did not dispute) that at least twenty files had been opened before the reinstallation but no longer existed on the laptop, indicating that they had been deleted before the reinstallation and then overwritten and rendered unrecoverable by the reinstallation. Doc. 214 at 32-33. Evans opined (and Protek again did not dispute) that the reinstallation required human intervention and was performed locally. *Id.* at 37; Doc. 178-2 at 6. Evans further opined that reinstalling an operating system is a common method of wiping information from a computer because it can cause the permanent destruction of data deleted prior to the reinstallation. Doc. 214 at 32-33, 37; Doc. 178-2 at 6. In sum, the record amply supports the conclusion that on March 28, 2016, when the laptop was in Williams's custody at his home, and after he had informed ACE of his intent to sue and been reminded of his preservation obligations, Doc. 89 at 10-11, 13-14, he deleted files and then reinstalled the operating system, thus wiping those files from the laptop.

Williams's denial of having reinstalled the operating system is not credible. In the face of the evidence just discussed, believing Williams's denial would require embracing one of his two theories, both of which amount to convoluted conspiracies that the record does not support. First, Williams submits that, more than a month before he returned his laptop to ACE, ACE rigged a second laptop to make it appear to be Williams's and reinstalled that laptop's operating

system to make it look like he performed the reinstallation; that after Williams returned his laptop, ACE switched the laptops' screens, putting the returned laptop's damaged screen on the rigged second laptop; and that ACE then sent the rigged laptop to D4 for a forensic analysis. Doc. 215 at 12-17. Second, Williams submits that ACE remotely accessed his laptop more than a month before he returned it to ACE; reinstalled its operating system (which may or may not have been possible to do remotely); and then sent the returned laptop to D4 for forensic analysis, adding some data (perhaps from his Indianapolis laptop) along the way. *Ibid.* The court finds credible the testimony from ACE witnesses denying that they did these things, and also finds credible Evans's testimony that the forensic evidence renders implausible Williams's theories.

As to the second ACE-issued laptop that Williams says he used in Indianapolis, the court finds that regardless how many laptops were formally *assigned* to Williams, *compare* Doc. 214 at 8 (Williams testifying that he had two), *with* Doc. 212 at 20, 88, 140-141 (Aldridge, Byland, and Landry testifying that, as far as they knew, nobody had more than the one laptop permitted by ACE policy), he *used* other laptops when he worked in the Indianapolis office, including at least one of the IT department's loaners, Doc. 214 at 8. But the court's siding with Williams on that factual dispute ultimately gets him nowhere.

To the extent Williams argues that the data no longer accessible on his home laptop was available to ACE all along because the data also was on the laptop he used in Indianapolis—and therefore that the destruction of that data on his home laptop was harmless because that data remained on the Indianapolis laptop—his argument fails for two separate and independent reasons. First, there is no evidence that any laptop in Indianapolis had on it the data that was deleted from Williams's home laptop. Rather, the only evidence of record, which is both uncontradicted and credible, is that Williams's remotely accessing his home laptop from

Indianapolis would *not* automatically have copied any files to the Indianapolis laptop. Doc. 214 at 119. Second, there is no evidence that ACE knew that Williams had saved relevant information on any laptop other than his home laptop. The court credits Byland’s uncontradicted testimony that: (1) ACE knew only about the laptop Williams kept at home and therefore preserved only that device; and (2) by the time ACE learned in Fall 2018, nearly two years after this case began, about the alleged second laptop, its search for additional laptops was fruitless. Doc. 212 at 142. Thus, even if data deleted from Williams’s home laptop also resided on his Indianapolis laptop, his failure for nearly two years to reveal in discovery the very straightforward and highly pertinent fact that he had an Indianapolis laptop deprived ACE of the opportunity to retrieve that data.

ACE’s lack of knowledge that Williams used other laptops in Indianapolis also undercuts—and is all but fatal to—his theory that ACE substituted an Indianapolis laptop for his home laptop when it sent the device to D4 for analysis. If ACE did not know that there *was* a second laptop until Fall 2018, it could not have reinstalled the operating system on that laptop in March 2016, waited until Williams returned his home laptop that May, swapped the screens, planted the files associated with Jacob Carey’s attempt to access the laptop, and then sent the second laptop to D4 in July 2017. And even if ACE were lying about its lack of knowledge—or had planted not only the evidence just described, but also the trail of Williams’s activity dating back to August 2015, the date of the first recorded activity by the “Triano.Williams” profile, Doc. 89 at 95; Doc. 214 at 35—framing Williams in this way would have required an incredible degree of clairvoyance. Or if not clairvoyance, the technical skill to backdate its activity without leaving a forensic trace, a possibility that finds no support in the record.

To support his switched laptop theory, Williams points to what he believes are three suspicious circumstances: (1) the failure to record the laptop's service tag on ACE's chain of custody form; (2) the ShellBag data indicating that someone used the laptop to access Gehring's and Holstein's network folders; and (3) the presence of Rubio's profile. None of that evidence makes Williams's theory even remotely plausible.

As to the first suspicious circumstance, ACE's documentation of the chain of custody was imperfect, to say the least. Much confusion could have been avoided had Aldridge photographed the service tag and recorded it on the chain of custody form. But Aldridge's and Evans's testimony were highly credible and support the conclusion that the laptop that ACE sent to Evans for analysis was the one that Aldridge received from Williams.

As to the second suspicious circumstance, Williams is correct that the ShellBag data suggests that *someone* accessed Gehring's and Holstein's network folders. Doc. 214 at 72-75. That data does not, however, speak to *who* accessed the folders, and it is thus too thin a thread on which to hang a finding that the laptop Evans analyzed was not Williams's home laptop but rather a loaner that Gehring and Holstein had used. That is particularly so given the uncontradicted evidence that the laptop automatically saved the profiles of any ACE users who logged into it, and neither Gehring's nor Holstein's profiles were found on the laptop—which means that neither of them used the laptop analyzed by Evans. Doc. 212 at 63, 187, 190; Doc. 214 at 12-13; Doc. 89 at 95. The only explanation supported by the record, then, is that Williams—as a systems administrator whose duties frequently included providing technical support—had used the laptop to access Gehring's and Holstein's network folders. Williams's testimony to the contrary is therefore not credible.

As to the third suspicious circumstance, the presence of Rubio's profile does not move the needle in favor of Williams's theory. The parties offered conflicting and inconclusive testimony as to when ACE switched from the image Rubio created to a new image, as to who made the new image, and as to whether the new image contained Rubio's profile. That said, the sum of the profiles on the forensic image cuts strongly against Williams's theory that the image was taken of a laptop that, as he described it, "was one of the ones [he] let people use" as a loaner. Doc. 214 at 8. Because each laptop automatically saved the profile of any user who logged in, Doc. 212 at 63, 187, 190; Doc. 214 at 12-13, the absence of anyone's profile other than Rubio's and Williams's strongly suggests that the imaged laptop was the one Williams kept at home, and not one that (by his own admission) he lent to others in the Indianapolis office.

That leaves Williams's remote installation theory. Nothing in the record suggests that it is even possible to reinstall an operating system remotely. Even if it were possible, Evans found no evidence of a remote reinstallation, Doc. 214 at 79, and Protek did not contradict that finding. ACE's ordinary method of remote access—TeamViewer—generated logs, but Evans found no logs indicating a connection to Williams's home laptop after February 1, 2016. *Id.* at 36, 44; Doc. 178-2 at 4. The only evidence Williams identifies to support his theory is Protek's UserAssist spreadsheet. Pl. Ex. 22. But Protek's report discusses that data without mentioning evidence of remote access, Doc. 169-2 at 3, and Evans credibly opined that the entry referring to "Remote Desktop Connection" meant only that a program with that name was run on the laptop *after* the reinstallation, Doc. 214 at 87-89.

In sum, the record overwhelmingly supports ACE's version of events and is inconsistent with Williams's version(s). The court therefore finds that Williams intentionally reinstalled the operating system on his ACE-issued laptop, resulting in the wiping and destruction of potentially

relevant information (the files he deleted before the reinstallation) “that should have been preserved in the anticipation or conduct of litigation.” Fed. R. Civ. P. 37(e). ACE further contends that Williams should be sanctioned for failing to suspend the auto-delete function on his email accounts, Doc. 86 at 2, but ACE did not press that theory in its closing argument at the evidentiary hearing, Doc. 215, and there is no need to address it because, as discussed below, Williams’s spoliation of the laptop’s data and his perjured testimony warrant dismissal on their own.

B. Willfulness

ACE also proved by a preponderance of the evidence that Williams’s spoliation was willful—in other words, not only that his reinstallation of the operating system on his ACE-issued laptop was intentional, but also that he knew that the reinstallation would destroy relevant data. As noted, Evans credibly testified that reinstalling an operating system requires affirmative user intervention and is thus not something that happens by accident, and that reinstalling an operating system is a common method of deleting information from a computer. Doc. 214 at 37. Given Williams’s experience as an IT professional, he must have known that reinstalling the operating system had the potential to overwrite—and thus render unrecoverable—previously deleted files. Indeed, nothing in the record suggests that reinstalling the operating system on a laptop Williams was about to return to ACE, his then-former employer, would have served *any* purpose other than destroying evidence.

Granted, there are more reliable and effective methods of destroying data on a laptop, such as physically destroying a hard drive or using professional tools to wipe data. But nothing in the record suggests that those alternative methods were comparable in terms of cost and likelihood of detection, which makes it unclear whether a person in Williams’s situation who wanted to destroy evidence would have chosen them. The existence of those alternatives thus

does not outweigh the evidence that Williams performed the reinstallation and that his aim was to destroy evidence. Viewing the record as a whole, ACE has proved by far more than a preponderance of the evidence that Williams reinstalled the operating system “with the intent to deprive [ACE] of the [destroyed] information’s use in the litigation.” Fed. R. Civ. P. 37(e)(2).

Further aggravating matters is that because Williams intentionally reinstalled the operating system, he must have known that he did so, which means that he repeatedly lied when he denied having done so at his deposition, Doc. 89 at 86 (p. 156, ll. 17-19), in his declaration, Doc. 180-15 at ¶ 4, and in his testimony at the evidentiary hearing, Doc. 214 at 147. Williams’s false deposition, declaration, and hearing testimony amounts to perjury.

“In the federal criminal context, perjury is defined as false testimony concerning a material matter with the willful intent to provide false testimony, rather than as a result of confusion, mistake, or faulty memory.” *Montano*, 535 F.3d at 565 (internal quotation marks omitted). Williams’s testimony satisfies each element of this offense: “false testimony,” “willful intent,” and “materiality.” *United States v. Savage*, 505 F.3d 754, 763 (7th Cir. 2007). The first and second elements necessarily follow from the finding that Williams intentionally reinstalled the operating system. Williams gave false testimony when he swore at his deposition, in a written declaration, and again at the evidentiary hearing that he did not reinstall the operating system, and he did so willfully because he was the person who performed the reinstallation. Under no imaginable circumstances would Williams have reinstalled the operating system, forgotten that he had done so, and then innocently offered an alternative theory in which ACE used the second computer (about which he had also “forgotten” until nearly two years into the litigation) to fabricate evidence of his misconduct.

As to the third element, Williams’s false testimony concerned a “material matter” in this litigation. *Montano*, 535 F.3d at 564. “[F]alse testimony is material if it is designed to substantially affect the outcome of the case.” *United States v. Galbraith*, 200 F.3d 1006, 1014 (7th Cir. 2000) (internal quotation marks omitted). Because “a lie influencing a pretrial issue will, in an attenuated sense, influence the ultimate outcome of the case itself, ... a falsehood told at a pretrial hearing is material if it is calculated to substantially affect the issue under determination at that hearing.” *United States v. DeLeon*, 603 F.3d 397, 403 (7th Cir. 2010) (internal quotation marks omitted); *see also United States v. Sanantonio*, 735 F. App’x 891, 892 (7th Cir. 2018) (“A lie calculated to influence a pretrial issue is material because it will influence the outcome of the case.”). Williams’s false denial goes to the heart of the issue presented by ACE’s sanctions motion, and given that ACE is requesting dismissal as a sanction, the motion plainly had the potential to determine the “ultimate outcome of the case itself.” *DeLeon*, 603 F.3d at 403. His false testimony therefore was material to the present motion. And as discussed below, because it cannot be determined which files Williams wiped from his laptop, yet because it is presumed that the wiped files were detrimental to his case, his false testimony almost certainly is material to the merits of his claims.

II. The Appropriate Sanction

ACE submits that the appropriate sanction is to dismiss Williams’s claims and to order him to pay its reasonable attorney fees and costs associated with investigating his misconduct and litigating its sanction motion. Doc. 86 at 19. Williams responds that dismissal is inappropriate because (1) he did not engage in any spoliation, and (2) there is no “record of delay or contumacious conduct,” prior sanctions, willfulness, bad faith, or fault. Doc. 124 at 15, 25 (quoting *Domanus v. Lewicki*, 742 F.3d 290, 301 (7th Cir. 2014)). Both arguments fail because, as shown above, Williams intentionally destroyed evidence and then repeatedly lied about it

under oath. Viewed as a whole, the record amply demonstrates that Williams “acted ... with a degree of culpability that exceeds simple inadvertence or mistake,” making dismissal an available sanction under both Rule 37(e)(2) (as to his destruction of data from his laptop) and the court’s inherent authority (as to his perjury). *Ramirez*, 845 F.3d at 776. Because Williams does not request a less severe sanction, he has forfeited any argument that dismissal is not the appropriate response under these circumstances. *See G & S Holdings LLC v. Cont’l Cas. Co.*, 697 F.3d 534, 538 (7th Cir. 2012) (“We have repeatedly held that a party waives an argument by failing to make it before the district court.”); *Alioto v. Town of Lisbon*, 651 F.3d 715, 721 (7th Cir. 2011) (“We apply [the forfeiture] rule where a party fails to develop arguments related to a discrete issue”); *see also King v. Ford Motor Co.*, 872 F.3d 833, 838 (7th Cir. 2017) (affirming the district court’s striking a declaration as a discovery sanction where the plaintiff “did not propose any alternatives to the district court”).

Even setting aside forfeiture, dismissal is the appropriate sanction. Recognizing that “the sanction of dismissal with prejudice must be infrequently resorted to,” the court has carefully considered whether a less serious sanction would be appropriate. *See Long v. Steepro*, 213 F.3d 983, 986 (7th Cir. 2000). The court also has evaluated Williams’s conduct in the context of the litigation as a whole to ensure that the “penalty [is] proportionate to the wrong.” *Ridge Chrysler Jeep, LLC v. DaimlerChrysler Fin. Servs. Ams. LLC*, 516 F.3d 623, 626 (7th Cir. 2008). Having done so, the court finds that Williams’s conduct warrants dismissal of his claims.

For starters, “[p]erjury committed in the course of legal proceedings is a fraud on the court,” *Allen v. Chicago Transit Auth.*, 317 F.3d 696, 703 (7th Cir. 2003), that itself “may warrant the sanction of dismissal” under the court’s inherent authority, *Montano*, 535 F.3d at 564. *See Rivera v. Drake*, 767 F.3d 685, 686 (7th Cir. 2014) (“[P]erjury is among the worst

kinds of misconduct.”). Williams also destroyed evidence “with the intent to deprive [ACE] of the [destroyed] information’s use in the litigation,” Fed. R. Civ. P. 37(e), and threw up a smokescreen of farfetched conspiracy theories in an effort to evade consequences for that misconduct. The result of that misconduct is a situation in which alternative sanctions—such as jury instructions and presumptions that the deleted information was unfavorable to Williams—cannot cure the prejudice to ACE because it is impossible to determine the full extent of the spoliation. Evans credibly opined that there is no way to know how many files Williams rendered unrecoverable by deleting files and then reinstalling the operating system, much less what those files contained. Doc. 178-2 at 3. The frequency with which Williams’s discovery responses directed ACE to the laptop he returned, combined with the commonsense assumption, built into Rule 37(e)(2), that parties who engage in intentional spoliation have something to hide, suggests that some of what Williams destroyed would have damaged his case.

Were it possible to pin the spoliation down to specific disputes—such as the timing of the creation and delivery of the ACE Culture Letter, for if the (now-lost) data showed that Williams created or delivered it *after* ACE announced that all IT staff would have to relocate to Indianapolis, his retaliation claim, which alleges that ACE forced him to move to Indianapolis in retaliation for sending the letter, would be mortally wounded—the prejudice to ACE could be cured by resolving those disputes in its favor. *See* Fed. R. Civ. P. 37(e)(2) (authorizing the court, upon finding that a party committed intentional spoliation of electronically stored information, to “presume that the lost information was unfavorable to the party” and to “instruct the jury that it may or must presume the information was unfavorable to the party”). But because there is no way to determine what data Williams destroyed and to which issues the data were relevant, there is no way to approximate the presumably unfavorable effect of that information, and thus no way

to craft instructions or presumptions that would eliminate—or even substantially mitigate—the prejudice to ACE. *See Leon v. IDX Sys. Corp.*, 464 F.3d 951, 960-61 (9th Cir. 2006) (affirming the district court’s dismissal of the plaintiff’s claims as a spoliation sanction where “any number of the [deleted] files could have been relevant to [the defendant’s] claims or defenses” and it was “impossible to identify which files and how they might have been used”). Although “the interests of justice are best served by resolving cases on their merits,” *Long*, 213 F.3d at 986, Williams’s intentional spoliation obfuscated the true merits of this case to the point where doing so is no longer a viable option, *see Leon*, 464 F.3d at 960-61.

That said, even if a sanction short of dismissal could cure the prejudice to ACE, dismissal of Williams’s claims would still be the sanction “proportionate to the wrong.” *Ridge Chrysler Jeep*, 516 F.3d at 626. Although Rule 37(e)(1) authorizes only “measures no greater than necessary to cure the prejudice” resulting from a party’s failure to take reasonable steps to preserve electronically stored information, Rule 37(e)(2) authorizes “further sanctions,” including dismissal, where the party “acted with the intent to deprive another party of the information’s use in the litigation.” *Barbera v. Pearson Educ., Inc.*, 906 F.3d 621, 627-28 (7th Cir. 2018) (internal quotation marks omitted). Likewise, “a district court’s inherent power to sanction for violations of the judicial process is permissibly exercised not merely to remedy prejudice to a party, but also to reprimand the offender and to deter future parties from trampling upon the integrity of the court.” *Salmeron*, 579 F.3d at 797 (internal quotation marks omitted).

Williams’s misconduct in destroying evidence was serious on its own. His attempt at a coverup—by committing perjury and generating a smokescreen of conspiracy theories to distract from the truth, and perhaps even to stick ACE with a default judgment, which he had the gall to request, Doc. 215 at 20-21—aggravated the situation still further. Although his efforts ultimately

failed, that failure came only after ACE was put to the time and expense of hiring a forensic expert, of researching and drafting its sanctions motion and extensive briefs, and of preparing for and participating in a two-day evidentiary hearing. *See Salmeron*, 579 F.3d at 797 (“[W]e do not require a district court to measure the impact on the litigation of a wrongdoer’s willful misconduct before it issues a dismissal sanction.”) (citation omitted). Taken as a whole, Williams’s misconduct was extraordinarily serious and warrants an equally serious response. Dismissing his claims enables the court to “remedy prejudice” to ACE, to “reprimand” Williams, and to “deter future parties from trampling upon the integrity of the court.” *Ibid.* (internal quotation mark omitted). An award of attorney fees and costs is warranted as well. *See Chambers*, 501 U.S. at 46 (“[I]f a court finds that fraud has been practiced upon it, or that the very temple of justice has been defiled, it may assess attorney’s fees against the responsible party, as it may when a party shows bad faith by delaying or disrupting the litigation”) (citation and internal quotation marks omitted); *Leon*, 464 F.3d at 955, 958-61 (affirming a dismissal sanction and attorney fee award where the district court determined the plaintiff employee “despoiled evidence by deleting 2,200 files from his [employer]-issued laptop computer during the pendency of the litigation”).

III. ACE’s State Law Counterclaim

Dismissing Williams’s claims leaves only ACE’s counterclaim for theft under Indiana law. Given that the parties are not diverse, Doc. 66 at ¶¶ 1-2, ACE correctly premises jurisdiction over its counterclaim on the supplemental jurisdiction, 28 U.S.C. § 1367(a). Doc. 29 at p. 31, ¶ 2. Section 1367(c)(3) provides that “[t]he district courts may decline to exercise supplemental jurisdiction over a claim under subsection (a) if . . . the district court has dismissed all claims over which it has original jurisdiction.” 28 U.S.C. § 1367(c)(3). “As a general matter, when all federal claims have been dismissed prior to trial, the federal court should relinquish

jurisdiction over the remaining pend[er]nt state claims.” *Williams v. Rodriguez*, 509 F.3d 392, 404 (7th Cir. 2007); *see also Dietchweiler ex rel. Dietchweiler v. Lucas*, 827 F.3d 622, 631 (7th Cir. 2016) (same). The general rule has three exceptions: “when the [refiling] of the state claims is barred by the statute of limitations; where substantial judicial resources have already been expended on the state claims; and when it is clearly apparent how the state claim is to be decided.” *Williams*, 509 F.3d at 404; *see also RWJ Mgmt. Co. v. BP Prods. N. Am., Inc.*, 672 F.3d 476, 480 (7th Cir. 2012).


None of the exceptions apply here. First, if this court relinquishes supplemental jurisdiction over ACE’s state law counterclaim, Indiana law would give ACE three years to refile it in state court. *See Artis v. District of Columbia*, 138 S. Ct. 594, 606 (2018) (citing Ind. Code § 34-11-8-1); *Hemenway v. Peabody Coal Co.*, 159 F.3d 255, 266 (7th Cir. 1998) (same). Second, substantial federal judicial resources have not yet been committed to the counterclaim. *See Davis v. Cook Cnty.*, 534 F.3d 650, 654 (7th Cir. 2008) (“[T]he district court disposed of the federal claims on summary judgment, and so ‘substantial judicial resources’ have not yet been committed to the case.”). And third, it is not clearly apparent how the counterclaim will be resolved. Given all this, relinquishing jurisdiction over the counterclaim is the appropriate course under § 1367(c)(3). *See Dietchweiler*, 827 F.3d at 631; *RWJ Mgmt. Co.*, 672 F.3d at 479-82.

Conclusion

ACE’s sanctions motion is granted. Williams’s claims are dismissed with prejudice, and Williams must pay the reasonable attorney fees and costs that ACE incurred in connection with uncovering Williams’s misconduct and litigating the sanctions motion. By September 30, 2019, ACE shall file a memorandum, with invoices and any other pertinent evidentiary support,

establishing its fees and costs. Williams has until October 21, 2019 to respond, and ACE may reply by November 4, 2019. ACE's motion to strike is denied as moot. The court exercises its discretion under 28 U.S.C. § 1367(c)(3) to relinquish its supplemental jurisdiction over ACE's state law counterclaim.

September 16, 2019



United States District Judge